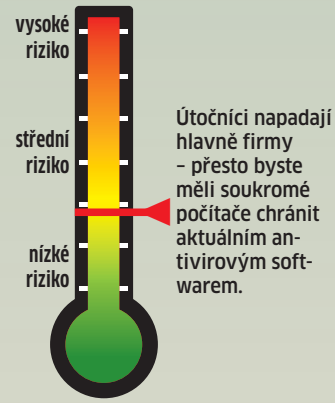
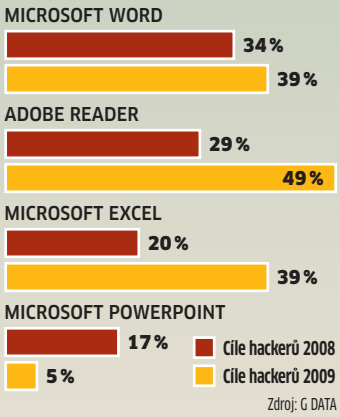
DATA A FAKTA

Barometr nebezpečí
v červnu:



Útočníci napadají hlavně firmy – přesto byste měli soukromé počítače chránit aktuálním antivirovým softwarem.

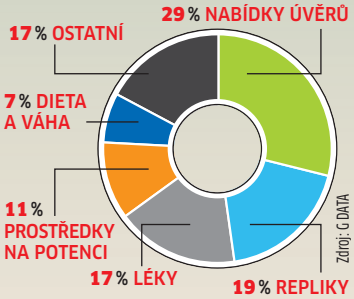
Hackeři milují PDF



Zdroj: G DATA

Nové preference: Během jednoho roku se zájem útočníků zřetelně posunul směrem k PDF.

Spammeři využívají krizi



Zdroj: G DATA

Q1/2009: K nejčastějším spamovým nabídkám patří špatné úvěry a falešné luxusní zboží.

Číslo měsíce

1 900 000

počítačů zahrnovala největší dosud odhalená hackerská síť botů, která se rozprostírala po 77 zemích.

Vlna útoků špičkových hackerů

Zveřejňují na webu zdravotní data, paralyzují letadla, odcizují **PŘÍSNĚ TAJNÉ PROJEKTY** – a vydělávají tak miliony.

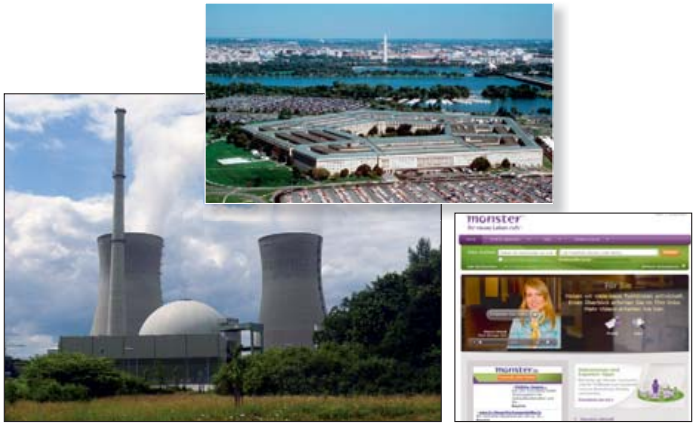
FABIAN VON KEUDELL

V aktuální řadě televizního seriálu „24 hodin“ manipulují hackeři řídicími systémy atomových elektráren, pozměňují letové trasy a získávají tajné vládní informace. V televizi však seriálový hrdina Jack Bauer vždy dokáže tomu nejhoršímu zabránit. A právě jeho by teď svět potřeboval ve skutečnosti, neboť realita už fikci dávno překonala.

Podle jedné z posledních zpráv amerického dozorčího úřadu pro letectví FAA (Federal Aviation Administration) hackeři v minulých letech několikrát pronikli do serverů FAA. Naposledy dokázali nejen získat přístup k osobním údajům 48 000 zaměstnanců, ale také servery odstavit. K tomu potřebné heslo správce získali útočníci pomocí „čenichacího“ nástroje (sniffer), který nainstalovali na doménové řadiče. Podle bezpečnostních expertů FAA už otázka nezní, zda hackeři někdy svou moc zneužijí, nýbrž kdy tak učiní – bezpečnost letového provozu by v takovém případě byla přinejmenším omezena.

Napadnutelná jsou dokonce i vysoce citlivá zařízení, jako atomové elektrárny. Bezpečnostní specialista Scott Lunsford se využitím slabého místa v softwaru SCADA (Supervisory Control and Data Acquisition) dostal do řídicích systémů elektráren. Oblíbeným cílem hackerů jsou také vládní firewally. Jak sděluje Pentagon, v současnosti denní počet skenů a útoků na servery amerického ministerstva obrany přesahuje 300 milionů. FBI a další úřady se samozřejmě snaží útočníkům a lidem v pozadí přijít na stopu – většina pachatelů ale zůstává neodhalena.

V poslední době se však vlna útoků začíná týkat i soukromých osob. Tak například hackeři pronikli do databanky jednoho z amerických úřadů, která obsahuje informace o receptech předepsaných více než osmi milionům pacientů. Databanku útočníci zašifrovali a za dešifrovací heslo nyní požadují výkupné ve výši 7,4 milionu eur a vyhrožují, že jinak údaje o pacientech zveřejní na internetu. V bezpečí nejsou ani data vedená na burzách práce. Nedávno padly do rukou datových špionů informace o některých uchazečích na webové stránce firmy Monster.



Datová loupež ve velkém stylu: Hackeři vydělávají ohromné peníze na špionážních zakázkách a manipulacích s řídicím softwarem.

Riziko „lidský faktor“: Hackeři často využívají slabá hesla

Při zabezpečování letového provozu a v armádě se nyní přechází na nové šifrovací servery – ty se však nedají nainstalovat přes noc. To, že hackeři na proniknutí do počítačových systémů ani nemusí vynakládat mnoho energie, mají často na svědomí slabá hesla a lidská selhání. Tak se nedávno na eBay objevily pevné disky obsahující důvěrné údaje z německých vyslanectví a data protiraketové obrany USA. Jack Bauer by měl v našem reálném světě práce až nad hlavu…

INFO: www.icann.org

VAROVÁNÍ FIRMY ESET

Okradení uživatelé a falešný antivirus

Služba Twitter, jedna z nejpoužívanějších sociálních sítí, čelí útokům, které mají pomocí sociálního inženýrství vylákat z uživatelů peníze za pořízení falešných antivirových programů. Podvodníci v rámci Twitteru hromadně zadávají své statusy pomocí klíčových slov, jako např. „Twitterbest“ a „Zasaden“, které jsou spojené s lákavými výrazy s pornografickým podtextem. Uvedené odkazy se aktuálně dostaly na přední místa v takzvaných Twitter Trend Topics – tedy mezi nejčastější výrazy, které v daném čase lidé použili ve svých statusech.

Klepnutím na odkaz, který má přiřazeno klíčové slovo (Twitter-Best.mp nebo Zasaden.mp), je uživatel přesměrován na falešné webové stránky obsahující škodlivý kód. Společnost ESET důrazně varuje uživatele, aby tyto stránky neotvírali – návštěvník je zpravidla vyzván k povolení aktualizovat aplikaci, např. přehrávač flash. Po odsouhlasení stažení se škodlivý software nainstaluje a uživatel obdrží falešné oznámení o infiltrování svého počítače. Poté se objeví nabídka na stažení aplikace „Fast Anti-Virus 2009“. Cílem útočníků je prodat falešný antivirus. Podle Juraje Malcha, vedoucího virové laboratoře společnosti Eset, představují falešné antivirové programy nebezpečí v tom, že mohou nezkušené uživatele připravit o značné peněžní částky. Tato forma škodlivého softwaru navíc obvykle obtěžuje uživatele vyskakovacími dialogovými okny, což značně snižuje produktivitu práce.

INFO: www.eset.cz

INFO

Nová bezpečnostní rizika

SYMANTEC ANTIVIRUS

Mezera v LogVieweru umožňuje útočníkům spouštět škodlivé programy. Stačí k tomu propašovat do počítače zmanipulovaný javaskript. Problém odstraňují nejnovější aktualizace produktů Symantecu.
INFO: www.symantec.com

F-SECURE

Chyba v rozpoznávacím mechanismu antivirových produktů firmy F-Secure způsobila, že program neidentifikuje žádné škůdce obsažené v archivech typů ZIP a RAR. Řešení je snadné – nainstalujte si aktualizaci od výrobce!
INFO: www.f-secure.com

MOZILLA FIREFOX

Předcházející verze 3.0.9 mohla u mnoha uživatelů přivodit zhroucení počítače. Příčinou je paměťová chyba, která také umožňuje propašovat do PC škodlivý kód. Ve verzi 3.0.10 už k haváriím počítače ani paměťovým chybám nedochází.
INFO: www.mozilla-europe.org/firefox

SUN SOLARIS XSCREENSAVER

Byla nalezena blíže nespecifikovaná chyba v Sun Solaris XScreenSaver (xscreensaver(1)), která může být zneužita k získání citlivých informací. Postižena může být platforma SPARC a x86. Dosud nebylo vydáno konečné řešení. Více informací naleznete na Sun.com (http://sunsolve.sun.com).
INFO: zpravy.actinet.cz

MICROSOFT OFFICE WEB COMPONENTS

Zranitelnost v této aplikaci umožňuje útočníkovi získat stejná práva, jako má aktuální uživatel. Aby bylo možné zneužít chyby, uživatel musí navštívit zasaženou webovou stránku. V současnosti se již objevují útoky, které se snaží zneužít této zranitelnosti. Opravení chyby se očekává se záplatami pro měsíc srpen, v současnosti je možné přijmout předběžná opatření, která naleznete na webu Microsoftu (**http://support.microsoft.com/kb/973472)**. Více informací a seznam zasaženého softwaru je na webu Microsoft.com **(http://www.microsoft.com/technet/security/advisory/973472.mspx)**.
INFO: zpravy.actinet.cz

MOZILLA FIREFOX

Byla nalezena zranitelnost v prohlížeči Mozilla Firefox, která může být zneužita ke kompromitaci systému. Zranitelnost je zavíněna chybou ve zpracování JavaScriptu používajícího HTML značky „font“ a její úspěšné zneužití může umožnit spuštění libovolného kódu. Zranitelnost je potvrzena ve verzi 3.5, ostatní verze mohou být také zasaženy. Více na serveru Secunia.com (**http://secunia.com/advisories/35798/**).
INFO: zpravy.actinet.cz

ADOBE COLDFUSION FCKEDITOR

Byla nalezena zranitelnost v Adobe FCKEditoru, který je součástí ColdFusion 8. Tato chyba dovolí vzdálenému útočníkovi uploadovat soubory do libovolných adresářů, což může vést ke kompromitování systému. Řešením je update na verzi 8.0.1 a aplikace hot fixu (více na **www.adobe.com/support/**).
INFO: zpravy.actinet.cz

MCAFEE

Ochranný software napaden

Mezera typu CSRF (Cross-Site Request Forgery) v bezpečnostním portálu „Secure“ firmy McAfee umožňuje útočníkům získat přístup k individuálním účtům klientů. Tento portál slouží provozovatelům webových stránek k otestování zabezpečení jejich vlastní stránky a při pozitivním výsledku jim vydá odpovídající osvědčení. Za normálních okolností má portál pomoci odhalit ve zdrojovém kódu stránky slabiny typu CSRF a SQL; výsledky testu pak bezpečnostní služba protokoluje v příslušném účtu. Pokud je však oběť útoku ke službě přihlášena a zároveň se při surfování v druhém okně browseru ocitne na zmanipulované hackerské stránce, mohou si útočníci načíst informace z bezpečnostního portálu. Tak přímo „z první ruky“ získají údaje o slabých místech ve webových stránkách postiženého. Tyto poznatky pak předávají dalším hackerům nebo je sami využijí pro vlastní útok. Nyní už firma McAfee tuto skulinu uzavřela. Přesto platí, že ani webové stránky s bezpečnostní pečetí nemusí být dokonale zabezpečené.

INFO: www.mcafee.com

GOOGLE

Viry v browseru

Provozovatel vyhledávače Google musel zacelit dvě kritické bezpečnostní mezery ve svém webovém prohlížeči Chrome. Jimi mohli útočníci do počítače dopravit a spouštět škodlivé programy. První mezera se týká interpretačního procesu. Hackeři zmanipulují bitmapová data tak, že v nich změní údaje o počtu pixelů v souboru – pak mohou útočníci spouštět programové kódy s oprávněním správce. Druhá mezera postihla grafickou knihovnu Skia 2D. Celočíselnou manipulací dokáží útočníci způsobit havárii prohlížecích panelů browseru nebo v jeho „sandboxu“ spouštět škodlivý kód. Pro Google je nepříjemné, že Skia 2D se používá i v mobilní platformě Android. Google právě testuje, zda mezera „funguje“ také v mobilních telefonech. Uživatelé Chrome by si měli browser aktualizovat na verzi 1.0.154.64.
INFO: www.google.com

MICROSOFT

Chyby ve Windows

Celých 23 bezpečnostních mezer ve Windows & Co. uzavřel Microsoft při posledním „patchday“– většinu z nich klasifikují v Redmondu jako kritické. Jak tvrdí bezpečnostní experti, updaty Microsoftu přišly hodně opožděně, neboť jimi softwarový gigant odstraňuje mezery známé už několik měsíců. Mezi nimi také chyby v Internet Explorer – prostřednictvím zmanipulované webové stránky bylo možné propašovat do počítače škodlivý program a spustit jej. Rovněž kritická mezera v Excelu, která umožňuje útočníkům získat přístup do počítače, byla uzavřena až šest týdnů po svém objevení. Za tu dobu už hackeři programovou chybu k proniknutí do počítačů využívali. A výrobce musel odstraňovat jednu slabinu dokonce i ve vlastním programovacím rozhraní WinHTTP.
INFO: www.microsoft.com

NOVÁ BEZPEČNOSTNÍ ŘEŠENÍ

Kaspersky Internet Security a Kaspersky Anti-Virus 2010

Společnost Kaspersky Lab oznámila vydání aplikací Kaspersky Internet Security 2010 a Kaspersky Anti-Virus 2010. Jedná se o novou generaci řešení, která mají ochránit domácí uživatele před počítačovými hrozbami. Nové verze produktů s číslem 2010 nabízejí výhody pokročilého systému prevence proti vniknutí (HIPS, Host-based Intrusion Prevention System). Tato technologie je součástí modulu Application Control (řízení aplikací), který přiřazuje bezpečnostní hodnocení dosud neznámým malwarovým programům. Součástí řešení je technologie Sandbox, která je příkladem virtualizační technologie a poskytuje vyhrazené zabezpečené prostředí pro běh aplikací. Inovativní služba Kaspersky Security Network využívá informace získané od milionů uživatelů řešení Kaspersky Lab, dramaticky snižuje dobu odezvy na nové hrozby a doplňuje reputační databáze o nejaktuálnější informace o neškodných i infikovaných souborech.

Kaspersky Internet Security: komplexní bezpečnostní řešení.

Kaspersky Anti-Virus 2010: Základní ochrana počítače.

Změny bezpečnostních hrozeb

„Ve světě se každý den objevují desítky tisíc nových škodlivých programů. Počítačová kriminalita se stala odvětvím s obratem mnoha milionů dolarů a stále exponenciálně roste. Běžné každodenní hrozby, jako jsou červi, trojské koně a viry, jsou postupně nahrazovány novými typy hrozeb. Do této skupiny patří například distribuované sítě kompromitovaných zařízení (zombie), které mohou zahrnovat až miliony počítačů. Samotný současný rozsah problému znamená, že konvenční metody, jako je heuristická analýza a řešení založené na definicích malwaru, už dnes nejsou schopné zajistit úplné zabezpečení. Nová povaha malwaru vyžaduje nové, komplexní metody ochrany. Řešení Kaspersky Internet Security 2010 z tohoto důvodu implementovalo revoluční přístup k ochraně, při němž je celosvětový monitoring nebezpečných aktivit prováděn přímo pomocí chráněných systémů a malware by do uživatelova počítače neměl vůbec proniknout," uvádí Eugene Kaspersky, výkonný ředitel společnosti Kaspersky Lab.

Bezpečné prostředí pro nové aplikace

Veškeré neznámé aplikace jsou pro zajištění bezpečnosti podrobeny analýze podle řady hledisek. Řešení Kaspersky Internet Security 2010 vytváří ještě bezpečnější prostředí, protože produkt integruje funkci Safe Run (bezpečné spuštění). Tato funkce je založena na technologii Sandbox, která představuje jednu z unikátních vlastností produktové řady Internet Security. Funkce Safe Run umožňuje uživateli spouštět nový software v izolovaném prostředí, které chrání operační systém před veškerými škodlivými změnami. Statistiky ukazují, že zranitelnosti v operačních systémech a důvěryhodných aplikacích mohou být hackery zneužívány k útokům na aplikace provedeným přes internet.

Funkce Safe Run nabídne bezpečnější a jednodušší surfování po internetu pomocí různých webových prohlížečů a navíc umožňuje současné spouštění libovolného počtu dalších aplikací. Zelené ohraničení kolem okna aplikace znamená, že aplikace je spuštěna v chráněném režimu.

Pro on-line hráče

Rozhraní nových produktů pro domácí uživatele od společnosti Kaspersky Lab prošlo rozsáhlou proměnou a je nyní podstatně přátelštější k začínajícím uživatelům. Do produktů Kaspersky Anti-Virus 2010 a Kaspersky Internet Security 2010 byl implementován režim automatizace aplikace, který volí nejvhodnější řešení bez toho, aby uživatele obtěžoval žádostmi o povolení akce tam, kde to není nutné. Zahrnuta je také samostatná možnost nastavení, určená pro fanoušky on-line her. Hráči rovněž mohou vypnout ty funkce, které ovlivňují internetový přenos a následně i dobu odezvy internetového serveru.

Zdokonalení Kaspersky Security Network

Vylepšení doznala také on-line reputační služba Kaspersky Security Network (KSN), která se

KASPERSKY

Utajené viry

Propašovat viry do počítače mohou útočníci pomocí zmanipulovaných PDF souborů. I když je v PC nainstalována antivirová ochrana firmy Kaspersky, skener nebezpečí nerozpozná a nechá škůdce projít. Podle bezpečnostního experta Thierryho Zollera je to dáno způsobem zpracování PDF souborů v antivirovém softwaru Kaspersky. PDF dokumenty začínají značkou „%PDF" a končí značkou „%%EOF". Data mezi nimi interpretují čtečky PDF jako dokument. Jestliže Kaspersky mezi oběma značkami objeví škůdce, ochranný software to ještě pozná, pokud však před značkami stojí ještě libovolný text, rozpoznávání selže. Kaspersky už zareagoval a nabízí opravu ve formě aktualizace softwaru. Jiní výrobci antivirového softwaru tímto problémem dosud postiženi nejsou.

INFO: www.kaspersky.com

poprvé objevila v předcházející verzi řešení Kaspersky Internet Security. Tato služba poskytuje vstup pro modul HIPS a je navržena tak, aby snížila dobu potřebnou pro detekci a zablokování nových typů hrozeb. Jakmile uživatel spustí program, služba ho porovnává se seznamem povolených aplikací (white list) a se seznamem Urgent Detection System (systém okamžité detekce) na serverech společnosti Kaspersky Lab. Stejně jako v předcházející verzi služba poté programu přiřadí jeho bezpečnostní ohodnocení. Služba KSN navíc nyní umožňuje modulu HIPS přesunout aplikaci z white listu sítě KSN do důvěryhodné skupiny.

Díky technologii KSN může mezi zjištěním dosud neznámého škodlivého programu a vytvořením plné ochrany pro uživatele produktů Kaspersky Lab uplynout méně než 40 sekund. To je do značné míry výsledkem ochoty uživatelů „domácích" produktů společnosti Kaspersky Lab, kteří se na službě Kaspersky Security Network rozhodli sami podílet. Přístup používaný touto službou je příkladem stále oblíbenějšího konceptu zabezpečení pomocí technologií cloud computingu. Potenciálně nebezpečné soubory nebo weby jsou v tomto případě kontrolovány on-line, namísto kontroly pomocí definic malwaru uložených lokálně na vlastním počítači.

Ochrana důvěrných dat

Rozšířena a vylepšena byla také sada nástrojů pro ochranu důvěrných dat. Nová generace produktů například automaticky zablokuje neopatrný přístup uživatele na známé phishingové weby. Blokuje i spyware určený ke krádeži uživatelských hesel a přístupových kódů. Řešení Kaspersky Internet Security nabízí i virtuální klávesnici, která uživateli umožňuje bezpečnější zadávání přihlašovacích jmen i hesel. Unikátní funkce chrání důvěrná data před krádežemi pomocí spywaru, přičemž mj. brání tomu, aby okno virtuální klávesnice mohlo být snímáno jako screenshoty, takže uživatelé mohou pracovat s on-line bankovnictvím nebo jinými důvěryhodnými informacemi ve zcela zabezpečeném prostředí. Vylepšeny a aktualizovány byly veškeré komponenty implementované v předešlých verzích produktu – včetně firewallu, nástroje pro heuristickou analýzu, modulu rodičovské kontroly a antispamu. Například antivirový modul nyní obsahuje emulátor skriptů, který umožňuje v reálném čase kontrolovat kódy v JavaScriptu nebo VB Scriptu, spouštěné při prohlížení různých webů. To je velmi důležitá inovace, protože podle odborníků společnosti Kaspersky Lab se dnes více než 70 % malwaru dostává do uživatelova počítače při návštěvě infikovaných webových serverů.

Vylepšený antivirový engine

Verze produktů s číslem 2010 je založena na vylepšeném antivirovém enginu, který nyní mnohem efektivněji detekuje škodlivé programy. I přes vyšší funkčnost si nové verze produktů zachovávají vysokou rychlost, a produkty dokonce v prostředí operačního systému Windows Vista dokáží provést široký rozsah úkolů až o 40 % rychleji než předcházející verze.

Kaspersky Anti-Virus 2010 a Kaspersky Internet Security 2010 jsou již v prodeji v Německu, ve Francii, Španělsku a Itálii. V červenci budou k dispozici také pro uživatele ve Velké Británii a v srpnu budou nabídnuty i v dalších zemích. Česká verze se chystá na konec prázdnin.

Řešení Kaspersky Internet Security 2010 a Kaspersky Anti-Virus 2010 lze zakoupit on-line na webových stránkách **www.kaspersky.cz** a **www.kaspersky.sk**.

VLC MEDIA PLAYER

Zranitelnost v přehrávači

V multimediálním přehrávači VLC byla nalezena zranitelnost zneužitelná ke kompromitaci systému. Zranitelnost je zaviněna chybou ohraničení. Zneužití může vyústit v přetečení vyrovnávací paměti například při otevření příliš dlouhé „smb://" URI. Zranitelnost se týká pouze verze pro OS Windows, potvrzena byla ve verzi 0.9.9, výskyt v ostatních verzích není vyloučen. Více informací naleznete na serveru Secunia.com **(http://secunia.com/advisories/35558/)**.

INFO: zpravy.actinet.cz

ZPRÁVA SPOLEČNOSTI ESET

Conficker je i nadále velmi aktivní

Pravidelná měsíční zpráva o nejrozšířenějších škodlivých kódech potvrdila stále vysoký výskyt červa Conficker. Systém Eset ThreatSense.Net v červnu označil Win32/Conficker jako nejrozšířenější hrozbu s podílem 11,08 %. Na druhém místě byl INF/Autorun, který ke svému šíření využívá přenosná (hlavně USB) média a který dosáhl podílu 8,33 % ze všech odchycených infiltrací. Oproti předešlému měsíci se nemění ani zbytek první pětky – třetí místo patřilo Win32/PSW.OnLineGames s podílem 8,24 %, čtvrté Win32/Agent (2,55 %) a páté obsadil INF/Conficker (2,10 %).

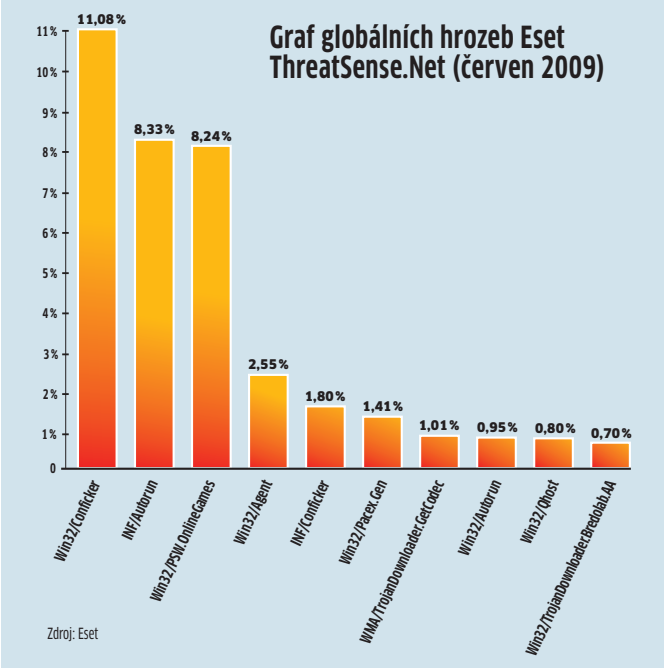
Novou hrozbou v rámci globálního žebříčku byl v červnu Win32/TrojanDownloader.Bredolab.AA. Tento malware se sám umisťuje do běžících procesů v počítači a snaží se vypnout bezpečnostní programy (uživatel o něm nemusí vůbec vědět). Je schopen se sám kopírovat do systémových souborů a spouštět se při každém zapnutí počítače. Zároveň komunikuje se vzdáleným serverem prostřednictvím HTTP. Pokud je tedy tento trojský kůň v systému, jeho hlavní úlohou je stahovat do infikovaného počítače další škodlivé kódy.

Evropa, Blízký východ, Afrika

Červen nebyl z pohledu rozšíření hrozeb v regionu výrazně odlišný od května. Win32/Conficker si drží první pozice v rámci východní Evropy a dominuje i v Itálii a nejnověji také ve Velké Británii.

V Polsku je už několik měsíců po sobě nejčastější hrozbou Win32/PSW.OnLineGames (13,9 %). Směs hlavně trojských koní útočících na hráče on-line her je kromě Polska jedničkou i ve Francii, a to s podílem 12,07 %. INF/Autorun je top hrozbou v Irsku (8,88 %), ve Velké Británii (7,04 %), v Litvě (5,75 %) a v Izraeli (5,68 %).

Česko i Slovensko mají v červnu na prvním místě stejnou počítačovou hrozbu. V obou zemích je nejrozšířenějším druhem malwaru Win32/TrojanDownloader.Bredolab.AA. V Česku dosahuje jeho podíl 7,22 %. V dalších zemích regionu je nejrozšířenější Win32/Conficker. V mnoha státech, kde je Conficker jedničkou, zároveň dosahuje velmi vysokých podílů mezi všemi detekovanými hrozbami: na Ukrajině 27,16 %, v Rusku 20,43 % a v Jižní Africe 16,60 %. Regionálními výjimkami jsou například Slovinsko, kde se uživatelé nejčastěji setkali s Win32/Qhost. Je to směs trojanů schopných prostřednictvím přesměrování DNS požadavků na server útočníka realizovat MITM (man-in-the-middle) útok. Útočník je tak schopen odchytit část komunikace infikovaného počítače.



ACTIVEX HROZÍ

Microsoft DirectShow s chybou

CSIS Security oznámila novou kritickou chybu v Microsoft DirectShow, která je současně aktivně zneužívána. Zranitelnost je způsobena chybou v komponentě ActiveX pro streaming video (msvidctl.dll). Úspěšný útok umožňuje spuštění libovolného kódu například při návštěvě zákeřné webové stránky. Zranitelná jsou Microsoft Windows 2000, 2003 a XP. Dosavadní radou je sledovat AV a IDS/IPS aktualizace výrobců a v případě výskytu nebezpečné ActiveX komponenty nastavit tzv. Kill Bit, který ji sice nechá nainstalovanou na počítači, ale znemožní Internet Exploreru ji volat. Více informací naleznete na serveru Tech Herald **(www.thetechherald.com)**.

INFO: zpravy.actinet.cz

ZRANITELNOST IPHONE

Odpojení od sítě

V současnosti je potvrzena chyba při zpracování SMS zpráv, která umožňuje odpojení iPhonu od sítě pomocí jediné zprávy. Dále se zkoumá, zda je možné chybu zneužít i ke spuštění kódu. Pokud by tomu tak bylo, jednalo by se o zatím nejzávažnější bezpečnostní chybu v iPhonu. Více informací naleznete na webu The Register **(www.theregister.co.uk/2009/07/02/critical_iphone_sms_bug/)**.

INFO: zpravy.actinet.cz

DIEBOLD

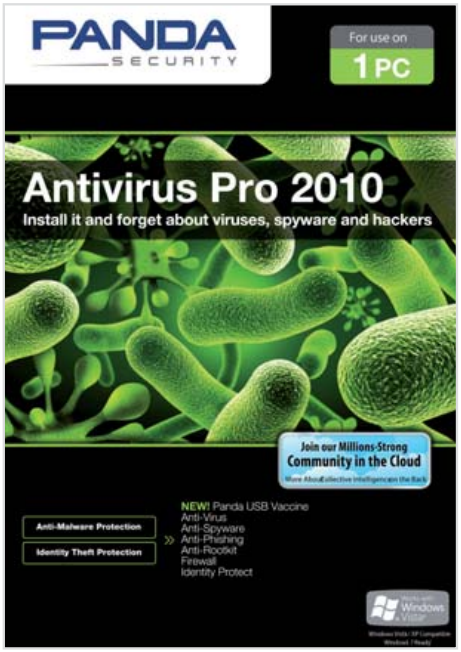
Napadené bankomaty

Pomocí trojského koně dokážou útočníci zmanipulovat peněžní automaty a získat tak údaje o účtech a čísla PIN. Výrobce bankomatů Diebold totiž u svých přístrojů používá jako operační systém Windows – bankomat je tak, jako každé jiné pécéčko, vystaven nebezpečí virového napadení. Jak tvrdí Vanja Svajcer z antivirové firmy Sophos, podařilo se hackerům propašovat do softwaru bankomatů trojského koně. Podle konkrétního modelu k tomu postačí už zmanipulovaná EC karta. K ovládání využívají podvodníci zcela prostě klávesnici pro zadávání PIN na samotném přístroji. Takto se dají čísla PIN i údaje o účtech všech transakcí jednoduše vytisknout na vestavěné tiskárně dokladů. Oběť nedokáže zvenčí manipulaci poznat. Sám výrobce se momentálně pokouší zvládnout situaci prostřednictvím aktualizace. V Německu jsou však už mnohé bankomaty předem ochráněny, neboť se u nich PIN zadává na speciální klávesnici, která komunikuje přímo se čtečkou karty.

INFO: www.diebold.com

NOVÝ BEZPEČNOSTNÍ SOFTWARE

Panda pro rok 2010



Na český trh přichází Panda Security s novými řešeními pro rok 2010. Mezi novinky patří Panda Antivirus for Netbooks, Panda Antivirus Pro 2010, Panda Internet Security 2010 a Panda Global Protection 2010.

Nové produkty jsou navrženy tak, aby nabízely ochranu s minimálním zpomalením počítače. Díky využití technologie „cloud computingu" dosahují nová řešení řady 2010 v porovnání s loňskými verzemi o 80 procent lepší výkon. Produkty Panda pro domácí uživatele také poskytují o 60 % vyšší rychlost při surfování a o 40 % vyšší rychlost stahování – opět ve srovnání s předchozími verzemi. V paměti pak zaberou pouze 8 MB.

Nová řešení od Panda Security také obsahují technologii chránící USB disky před virovými infekcemi a zabraňují šíření hrozeb, které běžně využívá malware. Další novinkou je zcela nová heuristická kontrola a společná databázi virů. A jaké výhody mají jednotlivé produkty?

Panda Antivirus for Netbooks je nové a nenáročné řešení pro zákazníky využívajícími netbooky a mini laptopy. Obsahuje antispyware, antiphishing, antirootkit, firewall a ochranu identity.

Panda Antivirus Pro 2010 chrání před viry, spywarem a hackery a obsahuje i nový modul ochrany před krádeží identity a zabudovaný firewall.

Panda Internet Security 2010 je komplexní řešení chránící před všemi typy hrozeb včetně virů, spyware, rootkitů, hackerů, online podvodů a krádeží identity a dalšími internetovými hrozbami. Jeho součástí je i systém záloh, spolu s prostorem na internetu o velikosti 2 GB. Součástí řešení je i rodičovská kontrola, která se stará o bezpečné používání webu dětmi.

Panda Global Protection 2010 je nejrozsáhlejší bezpečnostní řešení Panda Security, která chrání uživatele před všemi typy internetových hrozeb včetně virů, spywaru, rootkitů, hackerů, online podvody a krádeží identity. Kromě antispamové ochrany a rodičovské kontroly získávají uživatelé možnost zálohovat důležité soubory na DVD nebo online (do velikosti 5 GB) a v případě náhlé ztráty nebo poškození je obnovit.

PROBLÉMY S FILTROVÁNÍM INTERNETU

Pomáhají hackerům

Dokáže blokování webu zabránit šíření dětské pornografie? To nikdo neví. Víme však jedno: právě těchto blokád využívají hackeři ke svým cílům. Nepochybně to politici mysleli jen dobře: zablokováním některých webových obsahů se prostě pokusili znepřístupnit ilegální internetové stránky. Jenomže je v tom háček: tyto zábrany zneužívají hackeři ke špionáži v počítačích po celém světě.

Například v Číně jsou od 1. července 2009 schváleny k prodeji už jen počítače, které jsou vybaveny speciálním filtrovacím softwarem nazvaným „Green Dam". Ten zabraňuje přístupu na určité webové stránky, které obsahují například pornografický materiál. Vynalézaví hackeři však v softwaru objevili slabá místa, jejichž prostřednictvím mohou snadno získat přístup do počítače. Bezpečnostní mezera je přitom na počítači v podstatě předinstalována. S více než 250 miliony potenciálních obětí by tak útočníci mohli vybudovat až dosud největší síť botů – a ohrozit tak celý World Wide Web.

Nechtěné vládní pomoci se hackeři dočkali i v Německu v podobě blokování dětské pornografie. Jakmile speciální pracovní skupina Spolkového kriminálního úřadu (BKA) odhalí zakázanou webovou stránku, její IP adresu a webovou adresu zanese do seznamu blokovaných stránek. Ten obdrží poskytovatelé, kteří pak změní příslušné položky DNS (Domain Name System). Jakmile se nyní někdo pokusí vyvolat takto blokovanou stránku, dostane od Name Serveru nikoli korektní IP adresu webové stránky, ale namísto toho je přesměrován na informační stránku BKA.

To pochopitelně vyvolalo na veřejnosti značný rozruch, neboť to, které konkrétní stránky jsou blokovány a proč, vědí jen zasvěcení úředníci BKA. Na internetových fórech – a nejen na nich – se už proto projevují obavy z cenzury webu. Právě tuto nervozitu nyní využívají hackeři – a hned také nabízejí lákavé řešení: vlastní DNS servery, které surfaři mohou využít a blokování tak obejít. Mnozí uživatelé, kteří chtějí internetem brouzdat bez cenzury, pak tuto nabídku využijí, ačkoliv se trvale pohybují po legálních stránkách a s blokádou BKA by vůbec nepřišli do styku. Hackerský trik spočívá v tom, že „svobodné" DNS servery přesměrovávají legální, často využívané stránky na stránky hackerů. Kdo pak chce přes takový server například zkontrolovat svůj bankovní účet, ocitne se na phishingové stránce, k nerozeznání podobné originální stránce banky. Jakmile se přihlásí svými uživatelskými údaji, dá tak své osobní údaje na pospas hackerům.

CLIGS

Hackerské URL

Zkracovač webových adres Cligs dělá z dlouhých URL krátké. Například z **http://computer.shop.ebay.de/items/WLAN-Gerate tak vznikne URL www.cli.gs/wlan**. Tyto okliky však zmanipulovali útočníci a přesměrovali je na aktivistickou stránku. Postiženo tím bylo více než 2,2 milionu URL. Hackeři objevili bezpečnostní mezeru v administrační službě stránky a jejím prostřednictvím změnili cílové odkazy pro zkrácené adresy. V současné době je 93 % starých zkratek opět v pořádku a mezera je odstraněna. Poněvadž jsou však přesměrovávací služby často provozovány soukromníky, kteří na bezpečnost příliš nehledí, je jen otázkou času, kdy dojde k dalšímu útoku. Pro Firefox je nyní k dispozici plug-in **(www.longurlplease.com)**, který ukáže, co se za krátkou URL skrývá.

INFO: http://cli.gs

CANON SELPHY CP780

Kompaktní tiskárna fotografií

Společnost Canon rozšiřuje řadu kompaktních fototiskáren Selphy o nový model CP780 (nahrazuje starší CP760). Tiskárna byla navržena pro cenově dostupný tisk rodinných fotografií. Vytištění jedné fotografie netrvá ani minutu. Tiskárna se dodává v růžovém, modrém, stříbrném či bílém provedení a při použití napájecího akumulátoru na ní lze tisknout prakticky kdekoliv. Na tiskárně je 2,5" barevný TFT LCD displej, který umožňuje při tisku z paměťové karty prohlížení snímků a který také poskytuje stručné a srozumitelné instrukce. Selphy CP780 má tři otvory na paměťové karty, díky rozhraní PictBridge lze na této tiskárně tisknout i z většiny digitálních fotoaparátů a ve spolupráci s Bluetooth adaptérem navíc umožňuje tisk fotografií z mobilních telefonů a jiných bezdrátových zařízení. Technologie sublimačního tisku zajišťuje tisk lesklých fotografií s plynulými přechody tónů.
INFO: www.canon.cz

THINKPAD T400S

Odlehčený ThinkPad T od Lenova

Společnost Lenovo uvádí na trh nový notebook ThinkPad T400s. Ten vychází z předchozího modelu T400, je však téměř o 20 procent lehčí a má i řadu dalších vylepšení. Nový model našel inspiraci v nejtenčím a nejlehčím plně vybaveném notebooku ThinkPad X300 – ThinkPad T400s je tedy tenký (21 mm) a zároveň lehký (nejlehčí modely mají hmotnost pod 1,8 kg). Štíhlé konstrukce bylo dosaženo díky tenkému 14,1palcovému LED displeji, SSD disku a šasi Top Cover Roll Cage druhé generace, které společnost Lenovo poprvé představila právě u notebooku ThinkPad X300.
INFO: www.lenovo.cz

NAVIGON 8410

Navigace s realistickým zobrazením

Nový model 8410 produktové řady navigací Navigon nabízí realistické zobrazení města (funkce Foto Real City 3D) a ulic, přehrává filmy a je možné k němu dokoupit také televizní modul DVB-T. Foto Real City 3D realisticky zobrazuje domy, ulice a celé prostředí města včetně textur omítky domů, přechodů pro chodce i semaforů. V prvopočátcích je však samozřejmě možné očekávat tuto funkci jen u větších měst. Displej má úhlopříčku pět palců. Do Navigonu 8410 je integrován TMC přijímač. Mezi další funkce patří Panorama View (realistické zobrazení převýšení terénu), Landmark View (3D zobrazení památek), City View (zobrazení 3D modelů domů) a Clever Parking.
INFO: www.sunnysoft.cz